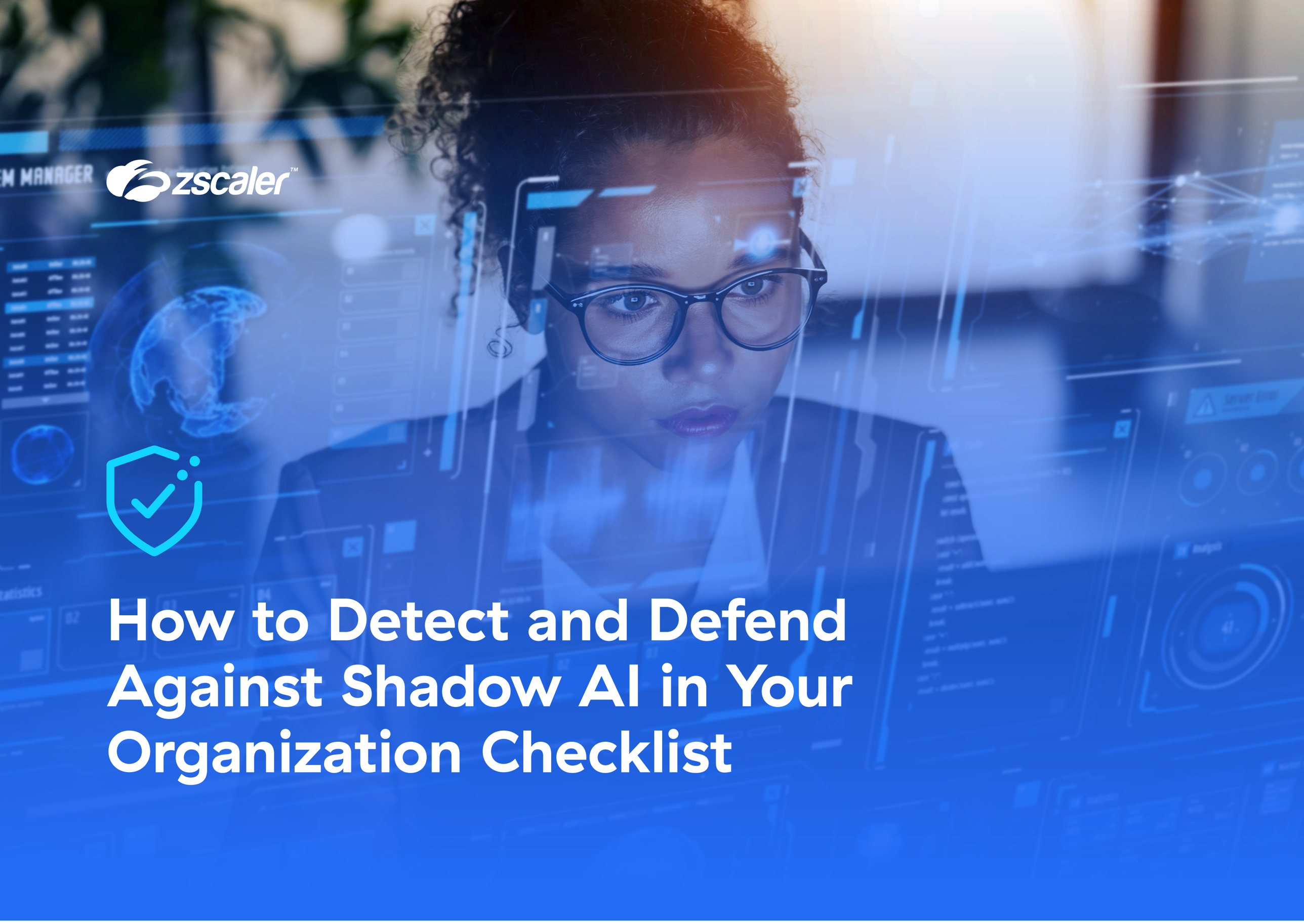

How to Detect and Defend Against Shadow AI in Your Organization Checklist

Generative AI (GenAI) is both reshaping how employees work and expanding the enterprise attack surface. While tools like ChatGPT, Gemini, Microsoft Copilot and Claude offer powerful productivity gains, their unsanctioned usage (known as Shadow AI) can quietly introduce serious data security and compliance risks.

Employees are increasingly turning to GenAI to generate emails, summarize documents or write code. But without IT oversight, they may inadvertently upload sensitive data like personally identifiable information (PII), financial records, or intellectual property to external artificial intelligence (AI) models that can't be controlled or audited. This makes data loss not just possible, but likely.

Rather than blocking GenAI tools altogether, which would hamper workforce productivity, many IT leaders are seeking effective ways to enable secure AI adoption that protects data without creating friction. Follow these six proactive steps below to identify Shadow AI activity across your environment, assess its risks and implement policy and technical controls—all while maintaining the benefits these applications offer.

01

Audit your Shadow AI exposure

- [ ] Before you can secure GenAI activity, you need to understand what's happening in your environment. Start by conducting a company-wide audit of third-party AI apps used by your employees, then identify those that haven't been approved by IT. Make sure to track traffic to GenAI tools, monitor unmanaged device access to these tools and evaluate the volume and types of data your workforce is sharing.

02

Evaluate your data risk footprint

- [ ] In many cases, employees turn to GenAI for speed and convenience without realizing the implications. Understanding the types of data your employees share with AI tools—and the reasons they do it—is essential for prioritizing your response efforts. Evaluate whether your workforce is sharing sensitive data like Personally Identifiable Information (PII), intellectual property, or financial records and map out the workflows where data enters these tools. You should also determine if your IT teams can control or recall the shared data, and identify if any compliance risks are being triggered as a result.

03

Create guardrails for GenAI use

- [ ] Establishing clear AI usage policies creates the foundation for responsible adoption across your organization. Define which GenAI apps are allowed and provide dos and don'ts to guide safe behavior for sharing corporate data with AI tools. Set expectations early by incorporating rules for AI-specific data handling into onboarding and security training and require all employees to acknowledge and follow these guidelines. Guardrails like these help protect data without blocking productivity.

04

Enforce security at the edge

- Strong policies need to be backed by enforceable controls. Monitor and control data flows to GenAI tools by deploying a modern security architecture like zero trust. Zero trust platforms incorporate several tools to help reduce data exposure, such as a cloud access security broker (CASB) to detect access to unauthorized AI apps, inline data loss prevention (DLP) to prevent employees from entering sensitive data into prompt fields, DSPM and AI-SPM to uncover shadow AI and reduce security and compliance risk to AI and data resources, browser isolation to block shadow AI use without disrupting web access and user and entity behavior analytics (UEBA) to detect anomalies in AI tool usage.

05

Detect and remediate Shadow AI risk

- Shadow AI often leads to risks like model-specific vulnerabilities, poisoning attacks, data exposure or data extraction and compliance violations, which can lead to financial, legal, and reputational damage. Organizations can deploy solutions like AI-SPM that continuously discover, detect and help remediate shadow AI security, compliance and operational risks. AI-SPM alerts when unmanaged AI models are detected, helps establish a risk assessment framework, policies, guardrails, remediation workflows, access controls, AI governance and more, ensuring secure AI operations.

06

Build a responsible AI culture

- Technology and policy are only part of the equation. It's just as important to build awareness across your organization. Educate your teams on the risks of sharing sensitive information with GenAI and offer examples of secure, appropriate AI usage. Explain how to use approved applications for AI-driven productivity and encourage employees to report unapproved tools or questionable behavior. Creating a culture of accountability helps turn your workforce into an extension of your security team.

07

Make Shadow AI management ongoing

- Securing your workforce's AI usage isn't a one-time project but an ongoing program that should evolve with the threat landscape. Keep your defensed up to date by continuously scanning and monitoring the environment for new GenAI tools, continuously monitoring the environment to block unsanctioned or inappropriate apps to eliminate shadow AI risk, tracking usage trends, blocking unsanctioned or inappropriate apps to eliminate Shadow AI risks and updating training content and policies to address emerging threats. Aligning your Shadow AI management effort with your organization's broader zero trust approach and DLP strategy ensures it remains a sustained effort rather than a quick fix.

Zscaler: GenAI security that checks all the boxes

When you implement the security measures outlined in this checklist, you'll establish a foundation that lets your organization confidently embrace GenAI without sacrificing security. This step-by-step approach gives your IT teams control over all aspects of GenAI use—from prompt inputs to acceptable apps—so your workforce can safely leverage AI-driven productivity.

The Zscaler Data Security Platform brings together protection across inline, cloud, and device data to unlock safe AI usage across your entire environment. With Zscaler, you get complete visibility and control over your employees' GenAI interactions with interactive dashboards, smart input prompt blocking, granular policy enforcement and more.

Want to see for yourself how Zscaler helps organizations secure AI use at scale? Book a demo of our AI data security platform or watch our product demo today.

Schedule a demo

Watch the product demo

zscaler™ | Experience your world, secured.™

About Zscaler

(NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com